

22



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,986	06/30/2000	Jin Su	10559/214001/P8707	1439
21552	7590	03/02/2005	EXAMINER	
MADSON & METCALF GATEWAY TOWER WEST SUITE 900 15 WEST SOUTH TEMPLE SALT LAKE CITY, UT 84101			SIMITOSKI, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2134	
DATE MAILED: 03/02/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/608,986

Applicant(s)

SU ET AL.

Examiner

Michael J Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 October 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 8-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 8-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. The response of 10/18/04 was received and considered.
2. Claims 8-27 are pending.

Response to Arguments

3. In light of Applicant's amendment to claim 12, the rejection of claim 12 under 35 U.S.C. §112 ¶1 set forth in the previous Office Action, is withdrawn.
4. In light of Applicant's amendments to claims 13, 14 & 23, the rejection of claims 13-15 & 23 under 35 U.S.C. §112 ¶2 set forth in the previous Office Action, is withdrawn.
5. In light of Applicant's amendment to claim 17, the objection to claim 17 set forth in the previous Office Action, is withdrawn.
6. In light of Applicant's amendment to claim 12, the objection to the drawings set forth in the previous Office Action is withdrawn.
7. Applicant's arguments filed 10/18/04 have been fully considered but they are not persuasive.
8. Applicant's response (p. 8, ¶1-3) argues that Schneier fails to anticipate the claim, as amended. However, this argument is moot in view of new grounds of rejection.
9. Applicant's response (p. 8, ¶4 – p. 10, ¶2) argues that Samar does not “teach or suggest saving the response as a named cookie”. Applicant is directed to Fig. 4 and col. 29, lines 1-19 of Elgamal, where Elgamal discloses a client verifying a server via certificates. Samar teaches a verifier (web/cookie server) authenticating a requesting entity (client), but rather than ending the process after the authentication, a security token/cookie is created and sent from the verifier to

Art Unit: 2134

the entity to be stored (the brownie + cookie is stored in the web server and the cookie is stored in the client) (§3.1 & Fig. 1). The web server challenges the cookie server; the cookie server responds to the challenge and stores the response as a named cookie (sends brownie + cookie back to the authenticating web server and the cookie is sent back to the browser) (Fig. 1 & §6.1). The cookie server also stores the cookie's reference data in its own database. This allows for fast authentication in the future (§1, ¶3, §3.1 & §6.1) because the stored response can be sent along with further requests. Cookies are well known in the art as a method to re-authenticate a requestor without having to perform a full authentication process. The modification of including a challenge from Elgamal's web server to the cookie server and saving the response as a named cookie would allow the web servers described by Elgamal to quickly authenticate the client in the future.

10. Applicant's response (p. 10, ¶3-7) argues that Schneier lacks "saving the response as a named cookie". However, as described above, Schneier is not relied upon for this feature.

11. Applicant's response (p. 10, ¶8 – p. 12, ¶2) argues that Schneier lacks "determining the client is a WinINET-based component" and that there is no motivation to combine Schneier, Alegre and Kristol to send "the encrypted key ... using a hypertext transfer protocol (HTTP) header." Alegre is cited for teaching including a session key in the cookie used for stated management. Kristol is cited for teaching that cookies are included in HTTP headers. The Kristol reference is a supporting reference for what is disclosed in Alegre. As applicant has pointed out, Kristol is stating that a risk is involved with sending sensitive data in the cookie in cleartext (this is what Alegre does), but the fact that Kristol suggests a suggested use does not preclude the combination from being made. Regarding Kristol's warning is simply a warning.

Art Unit: 2134

The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). In response to applicant's arguments against the Kristol reference individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

12. Applicant's response (p. 13) argues that the art of record lacks "saving the response as a named cookie". However, Applicant's is directed to the previous response regarding claim 8, for example where it is explained how Samar teaches the benefits of saving a response as a named cookie with an authentication token/cookie.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

14. Claims 14-15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification recites a

WinINET-based component, but does not define what attributes of a WinINET-based component differentiate it from other components.

15. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

16. Claims 14-15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 14 contains the trademark/trade name WinINET. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe Microsoft's Windows WinINET API and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2134

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claims 8-12, 16-22 & 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,657,390 to Elgamal et al. (Elgamal) in view of "Single Sign-On Using Cookies for Web Applications" by Samar.

Regarding claims 8 & 24, Elgamal discloses submitting a request to access a node (Fig. 12A), directing to submit a certificate (Fig. 4, client-hello), verifying the submitted certificate (col. 7, lines 20-40), performing a challenge (Fig. 4, client-hello) and generating a response to the challenge (Fig. 4, server-verify). Elgamal does not disclose saving the response as a named cookie. However, Samar teaches that storing response data (cookie id and cookie integrity check) (Fig. 1 & §6.1.2) is advantageous for single sign-on because no extra software has to be installed and it is independent from the authentication mechanism (§4). Samar teaches a verifier authenticating a requesting entity, but rather than ending the process after the authentication, a security token/cookie is created and sent from the verifier to the entity to be stored (§3.1 & Fig. 1). The web server challenges the cookie server; the cookie server responds to the challenge and stores the response as a named cookie (sends brownie + cookie back to the authenticating web server and the cookie is sent back to the browser) (Fig. 1 & §6.1). This allows for fast authentication in the future (§1, ¶3, §3.1 & §6.1) because the stored response can be sent along with further requests. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the authentication scheme used by Elgamal with the client-authenticating SSO architecture to store a response as a named cookie. One of ordinary skill in the art would have been motivated to perform such a modification to enable

Art Unit: 2134

single sign-on without the need for extra software or specific authentication mechanisms, as taught by Samar (Fig. 1 & §4). Elgamal, as modified, does not explicitly disclose verifying the submitted certificate with a trusted certificate, but discloses that the certificate is used to verify the authenticity of the server using well known techniques (col. 7, lines 20-40). The examiner takes Official Notice that retrieving a trusted certificate (self-signed certificate to obtain the authentic public key of a certificate authority) and verifying a submitted certificate based on the retrieved public key is old and well established in the art of cryptography as a method of securely authenticating an entity using a trusted third party. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the submitted certificate with a trusted certificate. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the submitted certificate via a trusted third party. This advantage is well known to those skilled in the art.

Regarding claims 9 & 25, Elgamal, as modified above, discloses using the cookie/response as a security token (Samar, §6.1).

Regarding claim 10, Elgamal, as modified above, discloses the security token being used to propagate initial authentication (Samar, §6.1).

Regarding claim 11, Elgamal, as modified above, discloses creating a connection session if the certificate is valid (Fig. 4 & col. 8, lines 54-61).

Regarding claim 12, Elgamal, as modified above, Elgamal lacks checking the certificate's signature with a trusted certificate, but discloses that the certificate is used to verify the authenticity of the server using well known techniques (col. 7, lines 20-40). The examiner takes Official Notice that retrieving a trusted certificate (self-signed certificate to obtain the authentic

public key of a certificate authority) and verifying a submitted certificate based on the retrieved public key is old and well established in the art of cryptography as a method of securely authenticating an entity using a trusted third party. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the submitted certificate with a trusted certificate. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the submitted certificate via a trusted third party. This advantage is well known to those skilled in the art.

Regarding claims 16 & 26, Elgamal discloses submitting a request to access a node (Fig. 12A), directing to submit a certificate (Fig. 4, client-hello), verifying the submitted certificate (col. 7, lines 20-40), performing a challenge (Fig. 4, client-hello) and generating a response to the challenge (Fig. 4, server-verify). Elgamal further discloses using the SSL library (col. 34, lines 39-49). Elgamal does not disclose saving a response as a named cookie. However, Samar teaches that storing response data (cookie id and cookie integrity check) (Fig. 1 & §6.1.2) is advantageous for single sign-on because no extra software has to be installed and it is independent from the authentication mechanism (§4). The web server challenges the cookie server; the cookie server responds to the challenge and stores the response as a named cookie (sends brownie + cookie back to the authenticating web server and the cookie is sent back to the browser) (Fig. 1 & §6.1). This allows for fast authentication in the future (§1, ¶3, §3.1 & §6.1) because the stored response can be sent along with further requests. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the authentication scheme used by Elgamal with the client-authenticating SSO architecture to store a response as a named cookie. One of ordinary skill in the art would have

Art Unit: 2134

been motivated to perform such a modification to enable single sign-on without the need for extra software or specific authentication mechanisms, as taught by Samar (Fig. 1 & §4).

Elgamal, as modified, does not explicitly disclose verifying the submitted certificate with a trusted certificate, but discloses that the certificate is used to verify the authenticity of the server using well known techniques (col. 7, lines 20-40). The examiner takes Official Notice that retrieving a trusted certificate (self-signed certificate to obtain the authentic public key of a certificate authority) and verifying a submitted certificate based on the retrieved public key is old and well established in the art of cryptography as a method of securely authenticating an entity using a trusted third party. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the submitted certificate with a trusted certificate. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the submitted certificate via a trusted third party. This advantage is well known to those skilled in the art.

Regarding claims 17, 18 & 27, Elgamal lacks creating a new authentication session with the authentication token. However, Samar discloses a centralized login server approach to single sign-on where an initial web server redirects a client to a new web server that has access to a cookie server (Fig. 2). The new web server then redirects the client back to the first server with the cookie where the web server verifies the cookie and returns a session cookie (creating and registering a new authentication session). The initial web server validates the new authentication session using the authentication token/cookie (Fig. 2 & §8). The benefit of the centralized login server is that all authentication information for the user is consolidated (§8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to

Art Unit: 2134

create and register a new authentication session. One of ordinary skill in the art would have been motivated to perform such a modification to enable the consolidation of all authentication information, as taught by Samar (Fig. 2 & §8).

Regarding claim 19, Elgamal lacks indicating a failure status to a client if verification fails. However, the examiner takes Official Notice that indicating a failure status (such as error messages) to a client if a verification/authentication, etc. fails is old and well established in the art of cryptography and network security as a means to notify a client that the verification has failed. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to indicate a failure status to a client if verification fails. One of ordinary skill in the art would have been motivated to perform such a modification to indicate to the client that verification has failed. This advantage is well known to those skilled in the art.

Regarding claim 20, Elgamal, as modified above, discloses the challenge being a random number (col. 7, lines 13-19).

Regarding claim 21, Elgamal, as modified above, discloses receiving an address/URL of a node and checking to determine if the address is protected (SSL to be used for information retrieval) (Fig. 12A).

Regarding claim 22, Elgamal lacks determining if the authentication token is already present. However, Samar teaches that SSO is useful so that users do not have to enter usernames and passwords many times per day (§1). Samar further teaches that in a centralized login server approach, a server first must check to see if a cookie was presented (authentication token already present) (§8 & Fig. 2) (otherwise the system would not be SSO). The centralized approach brings the benefit of authentication and management centrality (§8). Therefore, it would have

Art Unit: 2134

been obvious to one having ordinary skill in the art at the time the invention was made to determine if the authentication token is already present. One of ordinary skill in the art would have been motivated to perform such a modification to implement an SSO system to prevent repeated username and password combination uses, as taught by Samar (§1, §8 & Fig. 2).

19. Claim 13, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Samar, as applied to claim 8 above, in further view of Applied Cryptography, Second Edition by Schneier. Elgamal lacks generating a key, encrypting the key with a client's public key, sending an encrypted key to a client and using the encrypted key to encrypt communications. However, Schneier (page 48, § Key Exchange with Public-Key Cryptography) teaches generating a key/random session key (step 2), encrypting the key with a client's/Bob's public key (step 2), sending an encrypted key to a client/Bob (step 2) and using the encrypted key to encrypt communication (step 4). Schneier teaches that this is a basic key-exchange scheme used with Public Key cryptography to exchange a session key used to communicate securely (page 48, § Key Exchange with Public-Key Cryptography). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a key, encrypt the key with a client's public key, send an encrypted key to a client and use the encrypted key to encrypt communications. One of ordinary skill in the art would have been motivated to perform such a modification to exchange a session key to encrypt communications, as taught by Schneier (page 48, § Key Exchange with Public-Key Cryptography).

Art Unit: 2134

20. Claim 14, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Applied Cryptography, Second Edition by Schneier in view of Late Night ActiveX by Eric Tall. Schneier (page 48, § Key Exchange with Public-Key Cryptography) discloses generating a key/random session key (step 2), encrypting the key with a client's/Bob's public key (step 2), sending an encrypted key to a client/Bob (step 2) and using the encrypted key to encrypt communication (step 4). Schneier lacks determining if the client is a WinINET-based component. However, Tall teaches that WinINET API provides access to common Internet application-layer protocols like HTTP, FTP and Gopher and simplifies programming (p. 1, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine if the client is a WinINET-based component. One of ordinary skill in the art would have been motivated to perform such a modification to determine if the WinINET API can be used to ease programming, as taught by Tall (p. 1, ¶1).

21. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Tall, as applied to claim 14 above, in further view of U.S. Patent 6,199,113 to Alegre et al. (Alegre) in further view of "HTTP State Management Mechanism" by Kristol et al. (Kristol). Schneier teaches only a method of key exchange and therefore does not teach implementation details. Hence, Schneier lacks sending the key using a hypertext transfer protocol (HTTP) header. However, Alegre teaches that authentication data (cookie) can be stored at a browser to automatically authenticate a user during a session (col. 4, lines 1-7). Alegre teaches that a session key is stored in a cookie at the browser (col. 4, lines 31-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use

Art Unit: 2134

Schneier's key exchange protocol to exchange a session key and store it in the browser. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of automatically authenticating a user during a session, as taught by Alegre (col. 4, lines 1-54). Schneier, as modified, lacks specific disclosure of sending the key in an HTTP header. However, Kristol teaches that a cookie is transmitted via HTTP headers (§4.2) in HTTP state management. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to specifically send the key using HTTP headers. One of ordinary skill in the art would have been motivated to perform such a modification to set the cookie according to the HTTP/1.0 and HTTP State Management Mechanisms standards, as taught by Kristol.

22. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Samar, as applied to claim 22 above, in further view of Handbook of Applied Cryptography by Menezes et al. (Menezes). Elgamal discloses a system, as modified above, but lacks determining if a client is on an access control list if the authentication is present and valid. However, Menezes teaches that certificates should be revoked if evidence exists that suggests that the certificate should no longer be issued (§13.7.2). Menezes further teaches that certificate authorities publish certificate revocation lists to be checked for invalid certificates (§13.6.3) because distributed copies exist and may not immediately be aware of the need for revocation (§13.6.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine if the client/certificate is on an access control list/certificate revocation list after the authentication token is deemed valid (signature contained

in the certificate is successfully decrypted using the public key of the authority and compared to the data over which the signature has been taken). One of ordinary skill in the art would have been motivated to perform such a modification to make sure the distributed client certificate has been not revoked, as taught by Menezes (§13.6.3 & §13.7.2).

Conclusion

23. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:


(703)746-7239 (for formal communications intended for entry)


Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS
February 22, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100